REMARKS

Claims 1-26 and 28-29 remain in this application. Claims 1, 15, and 26 have been amended. No new matter has been added.

Independent Claims 1 and 26 have been amended to require obtaining or authenticating a digital transaction using "a delay number based on a delay time period between when a timing signal was transmitted from a remote source and when the timing signal was received," as suggested by the Examiner in a telephone interview. The Examiner is thanked for his suggestion. Claim 1 was further amended to require the environment information of the computer to include the delay number as well as data concerning the operating environment of the computer.

Independent Claim 15 has been amended to require the delay number as discussed above with reference to claim 1. In addition, claim 15 was amended to include obtaining a second delay number as well. The second delay number is then utilized as part of the environment profile to create the decryption key.

In addition, Independent claims 1, 15, and 26 have been amended to replace the word "generating" with "creating" to further clarify that a new key is created as opposed to being selected from a list of pregenerated keys. The encryption and decryption keys are actually newly created based on the environment information of the computer, which includes the "delay number." As illustrated in Fig. 12 of the application as filed, embodiments of the present invention append the environment information, in the form of an environment profile, to a user passphrase and then create a public and private key pair from the combined passphrase and environment information. (See application as filed page 35, lines 5-17, FIG. 12). Thus, if there are any changes to the environment information of the computer, the generated encryption key will change.

Once the encryption key is created, the file is encrypted. To access the file at a later date, a new key needs to be created as before. However, if there are any changes to the environment information of the computer, the created key will change, and thus be unable to decrypt the file. For example, if the encrypted file is moved to another computer, the environment information of the other computer will not match the environment information used to generate the encryption key

which was used to encrypt the file. As a result, when the other computer generates the new encryption key, the created key will not be able to decrypt the file, hence protecting the file from unauthorized access.

In view of these remarks and the above amendments, allowance of this application is believed to be in order, which action is respectfully requested. If any discussion of this application is initiated by the Examiner, please direct a call to **Joe A. Brock II, Esq., 909-758-5145.**

Respectfully submitted,
PATENT VENTURE GROUP
10788 Civic Center Drive, Suite 215
Rancho Cucamonga, CA 91730
(909) 758-5145
Fax: (888) 847-2501

By: _____
Name: Joe A. Brock II, Esq.
Reg. No.: 46,021

Date: May 13, 2005